U.S. FLEET CYBER COMMAND / U.S. TENTH FLEET

Labor Day 2014

You, the dedicated group of uniformed and civilian professionals who comprise the U.S. Fleet Cyber Command/U.S. TENTH Fleet world-wide team, work tirelessly to defend our nation 24/7/365. This is evident in the immense value you bring to Navy and Joint commanders, which will be measured based on our ability to:

- *Assure Navy command and control, networks and communications;*
- *Provide tailored signals intelligence (SIGINT) support to supported commanders and the National Security Agency/Central Security Service;*
- *Deliver effects in support of warfighting objectives;*
- *Create and share cyber situational awareness; and*
- *Provide certified Cyber Mission Forces to U.S. Cyber Command.*

Your work is making the difference in reaching these ends every day in the defense of not only our country but also of our allies and partners as you live the CNO's tenets: Warfighting First, Operate Forward, Be Ready. With the pace of operations, the necessarily classified nature of much of our work, and the quiet nature of the humble warfighter, however, we do not always have or take the opportunity to tell our family and friends how what we do protects them and our country.

This Labor Day weekend, if you are able to spend some time with family and friends, please consider sharing, however briefly, the accomplishments of the team you are part of; the articles below capture examples of our contribution around the globe. Our work is never done and continues every minute, of every hour, every day. I thank you for your dedicated service and please convey my admiration to your families for their sacrifices that make your service possible.

- Vice Adm. Jan E. Tighe, Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet
Fort Meade, Maryland, August 28, 2014

Navy Information Operations Command Texas (NIOC Texas)

NIOC Texas Navy Civilians and Sailors through personal initiative, technical expertise, and engaged leadership contributed to an astounding 70% increase in narcotics seizure in the U.S. Southern Command (SOUTHCOM) area of responsibility in just the first six months of calendar year (CY) 2014, versus the entirety of CY 2013; the results of which included seizure of over 70 metric tons (70,000 kg) of illicit narcotics, valued at over $2 billion.

- Our Sailors provided Force Protection (FP) and Indications & Warning (I&W) support onboard 10 US Navy, Coast Guard and allied maritime vessels and provided critical intelligence support that led to the seizure/disruption of over 16 metric tons of illicit narcotics (estimated street value of over $48 million).
- Surface Operations Sailors accumulated over 800 deployed days-at-sea and 210 days deployed to Joint Task-Force Guantanamo Bay, Cuba.
- Air Operations Sailors provided over 4,600 man-hours during 96 aerial reconnaissance flights in support of ground forces and SOUTHCOM tasking. These Sailors produced over 700 reports providing indications and warning in support of ground forces.

Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT)

NCTAMS LANT was established to combine the traditionally separate responsibilities of message traffic handling and data information management. Today, this combination of communications and computer technologies is key to ensuring the warfighter has access to the right information at the right time. Recent examples include:

- ♦ In June 2014, USS NEW YORK was the platform from which Special Forces launched an operation in Libya that resulted in the apprehension of Abu Khattala who is accused of orchestrating the assault on the American Consulate in Benghazi that resulted in the death of four Americans, including the U.S. Ambassador to Libya. The intelligence, coordination, and direction to execute the mission was conducted via Super High Frequency satellite links provided by NCTAMS LANT and our facility at Naval Support Activity Annex Northwest, Virginia. Khattala is currently standing trial for the assault.
- ♦ During the recent crises in the vicinity of Ukraine and Russia, U.S. Navy patrols have monitored the military activity on the Crimean peninsula and along the Russian/Ukraine border. The ships deployed to this area are dependent on satellite and data services provided to them from NCTAMS LANT and its stations in Europe.
- ♦ In the Syrian conflict, the U.S. Navy has maintained a presence in the region to deter the use of Weapons of Mass Destruction (WMD) and ensure the safety and defense of our interests in the region. These ships have been supported with satellite and data services from NCTAMS LANT, including direct support to MV CAPE RAY, which completed destruction of Syria's chemical arsenal earlier this month.

Navy Cyber Warfare Development Group's (NCWDG)

As the Navy's Center for Cyber Warfare Innovation, the NCWDG mission is to focus on the research and development of tactics to fill critical and challenging gaps in Fleet Cyberspace, enabling the Chief of Naval Operations and FCC/C10F to carry out cyberspace operations around the globe. Examples include:

- ♦ The Fleet Operations team testing advanced computer systems used to collect signals by deploying resources to various U.S. Navy ships, aircraft, and submarines to support warfighting objectives.
- ♦ The Cyber Effects team developed 10 Remote Control IED (RCIED) countermeasure devices and continuing to analyze and develop capabilities to defeat RCIEDs threatening U.S./Allied Forces in support of warfighting objectives.

Navy Cyber Defense Operations Command (NCDOC)

The NCDOC team of military and civilian cyber warriors process nearly 100 million sensor alerts each month to proactively mitigate threats and thereby assure the Navy's ability to command and control warfighting networks supporting Combatant/Fleet Commander missions worldwide.

- ♦ Our team of military and civilian cyber warrior's fight through an average of 300 suspected intrusions per month ensuring potential effects are rapidly mitigated before they negatively impact warfighting networks.
- ♦ Navy's cyber operating forces are rapidly evolving and employ cutting edge technology to effectively execute effects based Defensive Cyberspace Operations to proactively engage emerging global cyber threats.
- ♦ This includes employing over 200 boundary and nearly 400,000 host based sensors across its classified and unclassified networks to provide Attack Sensing and Warning of potential threats targeting our warfighting networks worldwide.
- ♦ Your Navy employs the most advanced cyber defense mission system in DoD to execute global network defense actions and support collaborative mission assurance, while providing Cyber Defense Battlespace Awareness to the warfighter.

Naval Satellite Operations Center (NAVSOC)

- ♦ NAVSOC operates, manages and maintains 13 assigned satellites, payloads and associated ground systems, providing 24/7 continuous, reliable, and endurable global narrowband, wideband and protected satellite communications to the Fleet, the Joint warfighter and Interagency teammates. NAVSOC, the world's first military Space Operations Command, continues in its 52nd year flying the nation's satellites.

Naval Computer and Telecommunications Area Master Station Pacific (NCTAMS PAC)

The NCTAMS PAC team of civilian and uniformed cyber professionals operate, maintain, and defend the Navy's portion of the Department of Defense Information Networks (DoDIN) in the Pacific and Indian Ocean area of operations supporting Fleet missions, afloat and ashore. As an example, NCTAMS PAC provides the following C4I network, telephony, and communications services:

- Network connectivity and services, to include web, email and chat, daily processing over 800,000 unclassified to Top Secret emails for 181 afloat commands and 250 coalition networked commands.
- Global Messaging with seamless delivery of 275,000 daily messages to 4,223 units.
- Telephony services to 180,000 subscribers across 16 regional sites.
- Globally connects Naval, Joint, Agency, and Coalition Forces through an average of 40 daily video teleconferences (VTCs).

U.S. Naval Computer and Telecommunications Station Far East (NCTS-FE)

NCTS-FE provides communications and information technology services for SEVENTH Fleet and supporting units, U.S. Naval Forces Japan, U.S. Naval Forces Korea, Defense Information Systems Agency and Japan Maritime Self-Defense Forces. The workforce is comprised of 230 military, 84 U.S. Civil Service, and 335 U.S. and Foreign contractor personnel.

- NCTS-FE provides Navy Enterprise Network (ONE-NET) services outside the continental U.S. on both the Non-secure IP Router Network (NIPRNet) and Secure IP Router Network (SIPRNet) to shore based and pier side units throughout the Far East region. ONE-NET is managed by the Theater Network and Operations Security Center (TNOSC), which oversees nine Local Network Service Centers (LNSCs) providing services to 26,000 network users via 16,000 workstations.
- NCTS-FE detachments provide the Commanding Officer with unique capabilities and mission sets. The detachments in Misawa and Okinawa are two examples. NCTS-FE DET Misawa provided Command, Control, Computer, Communication, and Intelligence (C4I) support to Commander, Patrol Reconnaissance Force Wing One (CPRW-1) for 145 operations and exercises this fiscal year to include ULCHI FREEDOM GUARDIAN, a joint Korean and U.S. exercise that trains partner nations and increases the joint response capabilities to a possible North Korean attack.

CTF 1030/Navy Information Operations Command Norfolk (NIOC Norfolk)

Commander Task Force (CTF) 1030 directs and coordinates operational and readiness support for four subordinate commands and 840 personnel in response to Commander, U.S. TENTH Fleet tasking. CTF 1030 provides tailored intelligence, planning, and personnel and equipment augmentation in support of Joint and Fleet exercises, work-ups, and deployments to ensure Navy cyber, electronic warfare, and information operations expertise in support of Fleet commanders worldwide. Specifically:

- We employ a team of Sailors and Civilians whose sole job is to accurately identify tens of thousands of hostile and friendly emitters and weapons to ensure U.S. Naval personnel on ships and submarines are equipped to properly detect, identify, and defend against attacks from air, sea, or land. These experts continually assess the threat environment world-wide keeping warfighters in other domains up to date with the latest information.
- The Navy Blue Team provides network security assessments to the Fleet and Navy commands ashore. Our Sailors deploy with Carrier Strike Groups and Amphibious Readiness Groups to serve as subject matter experts on ships defending the network from potential vulnerabilities and cyber-attacks. This helps assure the Navy's ability to provide command and control of its networks to carry out global missions.
- The Navy Red Team conducts cyber assessments in support of Fleet certification events and Combatant Command joint exercises. Our team of uniformed and civilian cyber experts ensure Fleet units are trained and certified in cyber operations before each deployment.
- Recently, the Navy Red Team participated in Exercise Rim of the Pacific, the world's largest international maritime warfare exercise, by simulating adversary action in the form of malicious network activity and social engineering manipulation to deliver operational cyber-effects to warfare commanders.

Navy Information Operations Command Pensacola

NIOC Pensacola established four Cyber Mission Force Combat Support Teams (CST) responsible for target development, target discovery and analysis, planning and synchronization, and intelligence in support of Combatant Command operations and war plans, enabling delivery of cyber effects against an adversary in cyberspace.

- NIOC Pensacola deployed 3 Sailors in support of Operation Enduring Freedom over the past year. These Sailors provided critical intelligence to drive Joint Special Operations Task Forces' missions focused on removing high value targets from the battlefield.

Navy Information Operations Command Sugar Grove (NIOC Sugar Grove)

NIOC Sugar Grove’s civilian and uniformed team supports the National Security Agency and Combatant Commanders directly engaged in Overseas Contingency Operations. Their watches led to the capture or kill of some the world's most wanted terrorists, thwarted potentially catastrophic terrorist attacks, and averted the unauthorized transfer of a highly capable military weapon system.

- Our Sailors provided more than 300 items of information, advancing key U.S. foreign policy objectives on four continents and supporting forward deployed combatant commanders in multiple theaters of operation.

Navy Information Operations Command Colorado (NIOC Colorado)

Embedded throughout the Aerospace Data Facility Colorado (ADF-C), NIOC Colorado Sailors manage $10 billion in national assets to provide 24/7 indications and warning support to National Decision Makers, Fleet and partner nation warships, and warfighters deployed throughout the world.

- Collaborating with the ADF-C's multi-service, multi-agency, and international work force allows for near real-time Force Protection (FP), Personnel Recovery (PR) support, Combat Search and Rescue (CSAR), advanced technical training curriculums, and all-source collaboration to meet Fleet and Joint requirements. We are the "*Eyes of the Fleet.*"

Naval Computer And Telecommunication Station San Diego (NCTS San Diego)

NCTS San Diego provides uninterrupted voice and data communications to the fleet and shore activities of the US Navy. Services include local base dial tone, commercial voice network access to local and long distance services for combatant commanders and emergency first responders (E911). Key users include the National Command Authorities, Combatant Commanders of the Unified Commands, and strategic and tactical subordinate commanders.

- Recently, the NCTS San Diego Team successfully provided voice and data communications support during FY14 RIMPAC for the Chilean Navy (CS Thomson and CNS Blanco), the Mexican Navy (ARM Revolucion and ARM Durango), and the Canadian Navy (HMCS Whitehorse and HMCS Naniamo).

Navy Information Operations Command San Diego (NIOC San Diego)

NIOC San Diego Sailors deploy as support teams to Carrier Strike Groups and Amphibious Readiness Groups to protect our ships from detection and tracking while operating throughout the world. NIOC Sailors:

- Train and assess Fleet Sailors in Computer Network Operations, Military Information Support Operations, Operations Security, Electronic Warfare, and Military Deception.
- Provide operational security, social networking, electronic warfare, and cyber awareness training to Sailors and their families.

Navy Information Operations Command Whidbey Island

Forward deployed Nodal Analysts assist in our support of fledgling democracies in the Middle East by employing Signals Intelligence in the protection of innocent civilians and provide the capability to respond with appropriate force as required.

- Signals Analysts on watch in Washington State and around the world maneuver throughout the communications spectrum 24 hours a day to derive the intent of our adversaries to aid decision makers.